Miercom

Lab Testing Summary Report

July 2009
Report 090708

Product Category:

Unified Communications

Vendor Tested:

CISCO

Products Tested:

Unified Communications Solution
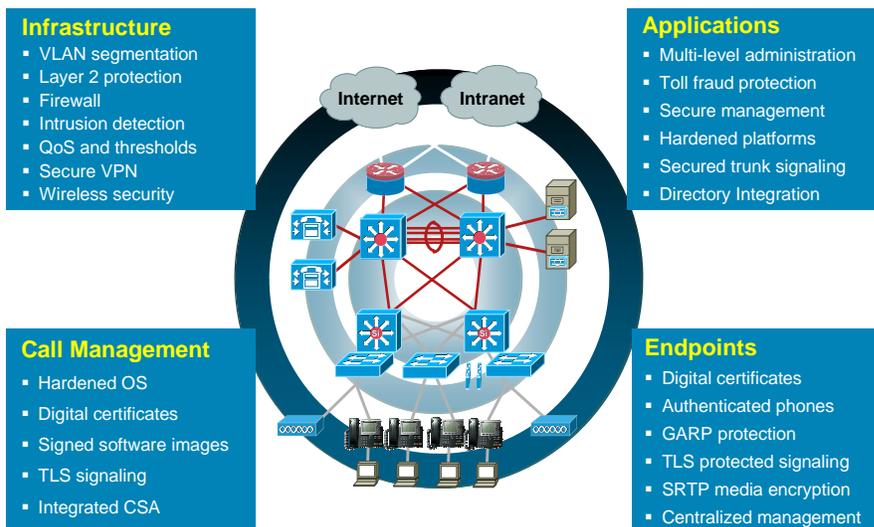
Miercom CERTIFIED SECURE

Key findings and conclusions:

- **Cisco Unified Communications solution uses multi-layered security to safeguard the enterprise**
- **Cisco Unified 7975 IP phone is resilient against DoS exploits, spoofing attacks, and protocol mutations**
- **Cisco ASA Phone Proxy successfully deploys secure phones without VPN tunnels or hardware**
- **Voice call quality was not affected with exploits and attacks directed at the Cisco ASA Phone Proxy**

Cisco Unified Communications Solution leveraging components from Cisco Unified Communications Systems Release 7.0 was evaluated by Miercom to assess the security of the system. Testing was conducted at the Cisco facility and Miercom lab. Specific areas examined included the ability of the Cisco UC solution to withstand numerous malicious attacks, resist voice and signaling traffic tampering, and limit unauthorized monitoring of network traffic, while successfully maintaining real-time voice communications. We analyzed the overall business benefits that the Cisco UC solution affords enterprise customers, while providing security.

Miercom performed numerous and varied attempts to gain surreptitious access to the Cisco UC solution. Penetration testing included representative scenarios to compromise the Cisco UC solution. We attempted to place unauthorized calls and to compromise and intercept VoIP communications, as a part of the planned attacks. By utilizing individual component security, as well as a system-wide security mechanism, the Cisco UC solution provides a multi-layered approach to safeguard the enterprise network. The Cisco UC solution incorporates security at each layer including endpoints, network components and the data center, as shown in Figure 1. This layered defense was proven effective to thwart our planned assaults. While providing a comprehensive Unified Communications solution, Cisco has embedded security throughout the system.

Figure 1: Cisco UC Security Layered Approach

Infrastructure
- VLAN segmentation
- Layer 2 protection
- Firewall
- Intrusion detection
- QoS and thresholds
- Secure VPN
- Wireless security

Applications
- Multi-level administration
- Toll fraud protection
- Secure management
- Hardened platforms
- Secured trunk signaling
- Directory Integration

Call Management
- Hardened OS
- Digital certificates
- Signed software images
- TLS signaling
- Integrated CSA

Endpoints
- Digital certificates
- Authenticated phones
- GARP protection
- TLS protected signaling
- SRTP media encryption
- Centralized management

Cisco UC solution successfully demonstrates a comprehensive layered security approach when defending and safeguarding enterprise networks. The Cisco UC Solution is rated Certified Secure by Miercom.

Test Bed Components
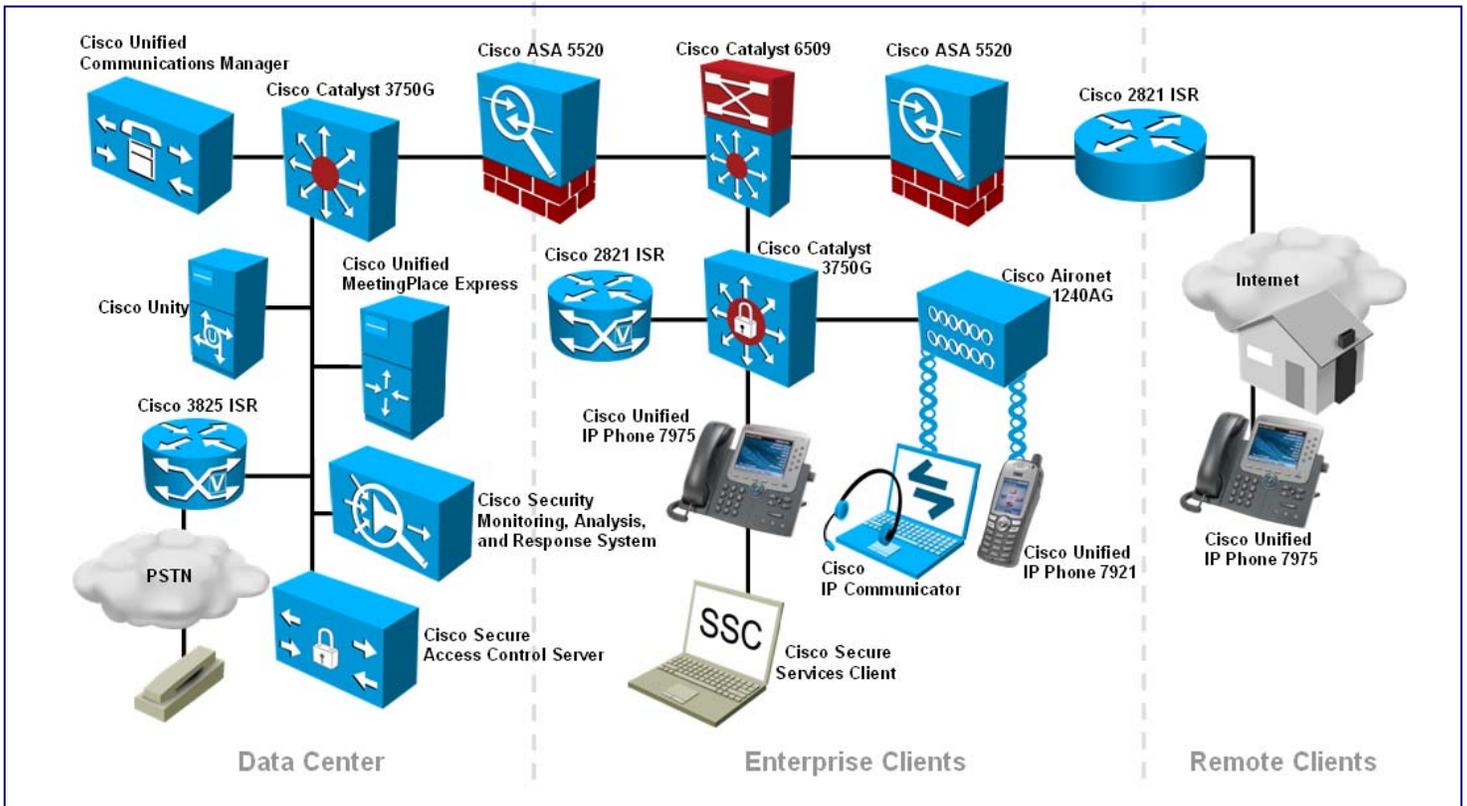
How We Did It

As shown in the diagram, the test bed represented a typical real deployment of the Cisco Unified Communications Solution using components of Cisco Unified Communications System Release 7.0 including IP Phones, with models for corporate office, mobile, and teleworkers. Core and edge switches; security firewalls; services routers; monitoring and messaging systems, Cisco Unified Communication Manager, Cisco Unity Server, Cisco MeetingPlace Express with a PSTN gateway to round out the Enterprise Network components. Network countermeasures were employed in multiple layers throughout the UC network.

We examined the internal configuration of the Cisco UC components via administrator (root) access in order to identify aspects of the deployed configuration that might cause weaknesses in the network defenses.

The tools used for port-scanning and enumeration included Nmap, Netcat and Nessus. SIP torture tests were conducted against the TCP stack. The endpoints were tested for any potential information leakage. In addition, attempts to gain surreptitious access were executed, along with attacks directed to the management interfaces (HTTP, SSH).

Penetration test tools were used to run attacks/exploits, security scans including protocol interaction with mutated traffic, published vulnerability exploit tests, Denial of Service (DoS), and SIP server torture tests (RFC 4475). We included proprietary test scripts and open-source security assessment products, and Backtrack 3 application. The Cisco Unified IP Phone 7975 was tested with 18,730 anomalies (generated from 528 variants). This evaluation was conducted using Miercom's own testing suite combined with Mu Test Suite (www.mudynamics.com) Mu-4000 Service Analyzer, performing security effectiveness assessments. The Mu-4000 Service Analyzer was also used to generate Denial of Service traffic with thousands of Transport and Network header variations on valid service-level traffic for protocols.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact reviews@miercom.com for additional details on the configurations applied to the system under test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a selection.

Layered Security Approach

Cisco Unified Communications Solution deploys security in multiple layers, starting from the phone endpoint to the core network. Cisco has security embedded within each component of the network infrastructure.

The distribution of the multi-layered security design provides a VoIP infrastructure that a sophisticated hacker assault team could not penetrate. Cisco proved it offers a secure Unified Communications Solution leveraging the built-in features of the IOS in the Catalyst switches, as well as native application security features in the Cisco Unified IP Phones and Cisco Unified Communications Manager.

With the addition of a properly configured firewall and security event manager, Cisco provided an additional layer of security to sustain a complete, secure Unified Communications solution, extremely resistant to compromise. Our exploit team was impressed with the security countermeasures Cisco employed and resiliency of the network.

Unified IP Phones

As a component of the layered security, the Cisco Unified IP Phone 7975 utilizes built-in security and phone hardening features. The Locally Significant Certificate (LSC) security feature provides enhanced security, allowing the user to have their own Public Key Infrastructure (PKI) and control their Certificate Authority, defining policies, restrictions, and usages on the generated certificates.

Transport Layer Security (TLS) encrypted and authenticated channel for call control is supported at the Cisco phone endpoints, with client certificates to provide secure signaling (SCCP or SIP). Call control is carried within 128-bit AES encrypted fields with RSA signatures for integrity. The implementation of SCCP over TLS prevents the capturing of parameters negotiated with the remote end.

The Cisco Unified IP Phone 7975 uses signed firmware, files and load images from Cisco Unified Communications Manager, preventing downloads of bogus firmware images or configuration files. Authorized downloads are verified by authenticating public key signatures.

The IP Phones can be securely administered and maintained from the Cisco Unified Communications Manager server. The administrator can specify call settings, enable or disable ports, and restrict or permit access using centralized tools, depending on the deployment of the IP phones over encrypted and authenticated channels.

Built into IOS

Cisco IOS software for the Catalyst access switches delivers an integrated set of security capabilities, and offers additional security throughout the UC network. In the Cisco UC solution tested, the phone and data connections/ports were directly connected to a Cisco Catalyst 3760G. This served as the access switch and the first line of defense against our attacks. A Cisco Catalyst 6509 served as the backbone switch during testing.

Dynamic Host Configuration Protocol (DHCP) snooping is an IOS security feature to combat against rogue DHCP servers and protect against DoS attacks. Network devices, like IP Phones are often configured to request their IP configurations from a DHCP server. A malicious computer can provide incorrect information, spoofing the real DHCP server, and allowing a man-in-the-middle attack to be launched. The DHCP snooping utility combats against rogue DHCP servers by using a DHCP binding table of authorized IP and MAC address

Auto-QoS is integrated in the IOS which simplifies QoS deployment and speeds provisioning over Cisco UC network. It enables Catalyst priority queuing for voice and data traffic, and provides SNMP and SYSLOG alerts for VoIP packet drops.

Traffic policing uses VLAN Access Lists (VACL) creating a Layer 3 type ACL, to provide deep inspection. Traffic policing limits the amount of traffic sent to the IP Phones. Traffic can be policed at an aggregate level port, per VLAN or per traffic flow. Traffic policing throttles DoS attacks when high volumes of traffic are flooded to the target node.

IP Source Guard is another security measure that prevents spoofing. It ensures the legitimacy of IP packets and MAC addresses, using the DHCP snooping binding to authorize IP and MAC addresses. This table also contains port number and VLAN information.

The Dynamic ARP Inspection (DAI) security application prevents Address Resolution Protocol (ARP) spoofing and man-in-the-middle attack, for both static and dynamic IP address, without requiring any changes on the end hosts. ARP requests are rate limited and are checked to ensure legitimacy. The IP Phones can be controlled and disabled if such malicious attacks are not countered.

Port security prevents Media Access Control Address (MAC) flooding attacks by limiting the number of MAC addresses that can appear on a port. Port security is configured on specific MAC addresses. The administrator can disable an offending port and phone either permanently, or for interim time period.

IEEE 802.1X

Cisco UC solution implemented IEEE 802.1X framework on Cisco Unified IP Phone 7975G to authenticate data end points prior to accessing the network. Traditionally, Cisco Discovery Protocol (CDP) is used to identify and determine parameters for Cisco Unified IP Phones and Catalyst switches. However, CDP does not identify PCs that are locally attached to the Cisco Unified IP Phone. Cisco Unified IP Phone 802.1X authentication allows a compliant endpoint to pass, through Extensible Authentication Protocol over LAN (EAPOL), messages to the 802.1X authenticator in the Cisco Catalyst switch. Only secure and compliant endpoints with valid credentials can access the network.

By using 802.1X enforced security policy compliance on all PCs, attack platforms seeking to access the network from Cisco Unified IP Phones were successfully thwarted. Access for Distributed Denial of Service (DDoS) attacks were unsuccessful.

System Hardening using Cisco Security Agent

Cisco Security Agent, a host based IPS security software, provides threat protection for servers and PCs. For the Cisco topology, we tested Cisco's Unified Manager and Cisco Unity Server with the Cisco Security Agent enabled. Cisco Security Agent incorporates security measures defined by the administrator.

Cisco Security Agent examines traffic, comparing it with pre-loaded attack signatures and events. Enabling Cisco Security Agent prevents attacks with malformed and mutated packets, monitors and enforces the applications that run on the server, detects port scans, prevents Trojan attacks and protects against SYNfloods DoS attacks.

Cisco Security Agent also prevents and protects against buffer overflow. These attacks add, insert, or replace the input of random bytes causing buffer overflows. We verified that these potential integer overflow conditions did not cause buffer overflows. Execution of malicious code in the data and stack space was prevented.

Port scanning and enumeration are used to detect opened, filtered or closed ports. Cisco Security Agent logs, correlates and reports these scans to detect anomalies.

Cisco Security Agent also detects and drops malformed packets and malicious executables, before they enter and can affect the operating system.

Cisco Adaptive Security Appliances (ASA)

Cisco used the ASA 5500 Series Adaptive Security Appliances, a multi-function security appliance as both a firewall and remote access device.

The Cisco ASA functionality was used for additional protection from attacks and to control allowable data center traffic. The Cisco ASA was also used as a phone proxy, to deploy secure phones without the need for VPN tunnel or hardware.

The ASA firewall functionality has several enhanced features, offering threat defense and secure communications services. The stateful inspection feature operates at a higher performance level compared to Layer 3 packet filtering. It records and maintains a state table which contains the source, destination address, port numbers, TCP sequencing information and additional flags for each TCP/UDP connection associated with that session.

Rate limiting feature assigns bandwidth restriction to traffic, limiting flooding traffic in a DoS attack. Rate limitation also performs policing, queuing, and congestion control.

Stateful application inspection ensures the secure use of SCCP and TFTP applications and services. Network Address Translation (NAT) is used to identify the location of embedded addressing information. NAT then translates these addresses and updates any fields that are affected by the translation. The SCCP and TFTP inspection monitors these sessions, identifies the dynamic port assignments, and permits data exchange for a specific session.

The anti-spoofing feature protects interfaces from IP address spoofing by creating filters, and confirming source address and route integrity. If the source address or the route is considered to be a suspect, the packet is dropped, and IP spoofing is used to disguise the true IP address source of the attacker.

Cisco TLS Proxy feature inspects encrypted signaling and media traffic and provides secure inter-working between the firewall and encrypted voice calls. The ASA also enables a single remote access platform to secure the deployment of remote phones using Phone Proxy.

Bottom Line

Cisco proved not only to have a very effective unified communications solution, but also, an extremely resilient and secure communications solution. Cisco has achieved the Miercom Certified Secure Certification, which is the most challenging and comprehensive security assessment in the industry.

By utilizing all the security features available, the Cisco Unified Communications Solution is hardened to deflect security threats. Network defense was effective in thwarting all of our assaults, which have compromised other UC solutions on the market.

Miercom examined the Cisco Unified Communications Solution with countermeasures deployed. Cisco UC Solution has exceeded Miercom's security certification standards.

Miercom Certified Secure

Based on hands-on penetration testing and security vulnerability assessment, the Cisco Unified Communications Solution is Rated Certified Secure in the 2009 Miercom Unified Communications Security Industry Assessment. This rating is based on the specific testing in those areas described in this report as well as other tests that were conducted.

The award is in accordance with the Certified Secure Testing Program of Miercom, effective for one year from test certification. The Certified Secure program recognizes products that exhibit exceptional qualities in specific test criteria when analyzed in a competitive test review or Miercom Industry Assessment.

Cisco's multi-layered security design proved that it provides a secure UC solution, leveraging features of Cisco IOS, Catalyst switches, enhanced security features in the Cisco Unified IP Phones and Cisco Unified Communications Manager.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
www.cisco.com
1-800-553-6387

About Miercom's Product Testing Services

With hundreds of its product-comparison analyses published over the years in such leading network trade periodicals as Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony and other leading publications, Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.